APPLICATION FOR A UNITED STATES PATENT

UNITED STATES PATENT AND TRADEMARK OFFICE

(MBHB CASE No. 01-469; 3Com Case No. 3727.CS.US.P)

Title: **SYSTEM AND METHOD FOR MANAGING FOREIGN AGENT SELECTIONS IN A MOBILE INTERNET PROTOCOL NETWORK**

Inventors: Gregory K. Lewis, a citizen of United States, and a resident of San Diego, CA;

Frederick J. Dickson, a citizen of the United States, and a resident of San Diego, CA; and

Abhishek Sharma, a citizen of India, and a resident of Mt. Prospect, IL.

McDonnell Boehnen Hulbert & Berghoff
300 S. Wacker, 32 Floor
Chicago, IL 60606

Assignee: 3Com Corporation
5400 Bayfront Plaza
Santa Clara, CA 95052

Express Mail No.: EL604648551US
Date of Deposit: June 14, 2001

Docket # 3727.CS.US.P

COMPUTER PROGRAM LISTING APPENDIX

This application contains a computer program listing appendix on a compact disc, which is fully incorporated by reference, in compliance with 37 C.F.R. § 1.52(e). The compact disc contains a single file named "Appendix.txt" of size 127,621 bytes created on June 14, 2001.

COPYRIGHT

A portion of the disclosure of this patent document contains material that is subject to copyright protection. The copyright owner has no objection to the facsimile reproduction by anyone of the patent disclosure, as it appears in the Patent and Trademark Office patent files or records, but otherwise reserves all United States and International rights whatsoever.

FIELD OF THE INVENTION

The present invention relates to communications in mobile Internet Protocol ("IP") networks. More particularly, it relates to providing a centralized node for managing foreign agents in such networks.

BACKGROUND OF THE INVENTION

Public packet switched networks can be used to carry traffic to and from a mobile communications device (a mobile node), such as a mobile host, or router that changes its point of attachment from one network to another. The basic architecture of mobile IP data networking is known in the art and described in several publications, including the Request for Comments ("RFC") document RFC 2002 (1996) (hereinafter "RFC 2002"), which is currently available from the Internet Engineering Task Force ("IETF") at www.ietf.org for more information. Persons skilled in the art of mobile IP data networking are familiar with that document and devices used to implement mobile IP data networking in practice.

In a mobile IP communication network, a mobile node communicates with a target host on an IP network by means of two devices, a "foreign agent" and a "home agent". One example

McDONNELL BOEHNEN
HULBERT & BERGHOFF
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

of a mobile IP network that describes that type of communication is presented in U.S. Patent Application Serial No. 09/354,659 entitled "Mobile Internet Protocol (IP) Networking with Home Agent and/or Foreign Agent Functions Distributed Among Multiple Devices," the entire content of which is incorporated herein by reference. Typically, the foreign agent functionality is incorporated into a router on a mobile node's visited network. The foreign agent provides routing services for the mobile node while it is registered with the home agent. For example, the foreign agent de-tunnels and delivers datagrams that were tunneled by the mobile node's home agent to the mobile node.

The home agent is typically incorporated into a router on a mobile node's home network. The home agent maintains current location information for the mobile node. When one or more home agents are handling calls for multiple mobile nodes simultaneously, the home agents are providing, in essence, a service analogous to a virtual private network service. Each mobile node is typically associated with a separate home network and the routing path from that home network, through the home agent, to the foreign agent and mobile node is like a virtual private network for the mobile node.

Mobile IP requires link layer connectivity between a mobile node (a mobile entity) and a foreign agent. However, in some systems the link layer from the mobile node may terminate at a point distant from the foreign agent. Such networks are commonly referred to as third generation wireless networks. Figure 1 is a block diagram illustrating a network architecture that is typically employed in the third generation wireless networks. Referring to Figure 1, a mobile node 10 communicates with a target host 34 on an IP network 30 by means of three devices, a radio network node 16, a packet data serving node 18, and a home agent node 24. The physical layer of the mobile node 10 terminates on the radio network node 16, and the foreign agent's functionality resides on the packet data serving node 18. Typically, the radio network node 16

McDONNELL BOEHNEN
HULBERT & BERGHOFF
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

relays link layer protocol data between the mobile node 10 and the packet data serving node 18, and the packet data serving node 18 establishes, maintains and terminates the link layer to the mobile node 10. For example, the mobile node 10 may be linked to the radio network node 16 via a communication link on a radio access network.

The packet data serving node 18 provides routing services for the mobile node 10 while it is registered with the home agent 24. The packet data serving node 18 de-tunnels and delivers datagrams that were tunneled from the home agent node 24 via an IP network 20 to the mobile node 10. The communication traffic exchanged between the packet data serving node 16 and the home agent 24 includes data traffic as well as control traffic. The control traffic includes registration request or registration reply messages. The control traffic terminates at the home agent 24 and the packet data serving node 16, while the data traffic is routed between the mobile node 10 to the target host 34. The target host 34 may be connected to a home network 26 by any number of networks, such as the IP networks 20 and 30, or it may be directly located on the home network 26. Alternatively, the target host 34 may be connected to the home network by other types of packet switched networks.

The home agent 24 may be implemented on a router on the mobile node's home network 26. The home agent 24 maintains current location information data for the mobile node 10 such as foreign agent address, mobile home address and a secret key shared between the home agent and the mobile node. The home agent tunnels data from the target host 34 to the packet data serving node 18, and similarly provides tunneling services in the reverse direction. More information on point-to-point tunnels, such as a Layer 2 Tunneling Protocol ("L2TP") tunnel may be found in the RFC 2661, currently available at www.ietf.org. The home agent 24, therefore, typically implements at least two distinct tasks for the mobile node 10. First, the home agent 24 performs a registration and authentication process to determine whether the mobile

McDONNELL BOEHNEN
HULBERT & BERGHOFF
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

node 10 is authorized to access the home network 26. This may involve, for example, checking the identification of the mobile entity, such as through the use of the mobile entity's unique serial number or manufacturing number, password authentication, and possibly checking whether the mobile entity's account is current and paid. The home agent's registration and authentication function may be performed in conjunction with, or with the assistance of, a second device, such as an authentication, authorization and accounting server such as a Remote Authentication Dial-In User Service ("RADIUS") server. More information on a RADIUS server may be found on in the RFC-2138, which is currently available at www.ietf.org for more information. As is known to those skilled in the art, the registration process includes receiving and processing registration request messages from the packet data serving node 18 and sending registration reply messages to the packet data serving node 18.

Similarly to the home agent 24, the packet data serving node 18 also performs two distinct tasks for the mobile node 10. The packet data serving node 18 handles registration and session control for the mobile node 10, including sending registration request messages to the home agent 24 and processing registration reply messages received from the home agent 24. Additionally, the packet data serving node 18 has tunneling responsibilities for forwarding data packets to the home agent 24 for ultimate transmission to the target host 34, as well as de-tunneling data from the home agent 24 for ultimate delivery to the mobile node 10. Further, the packet data serving node 18 provides authentication, authorization and accounting services for the mobile node 10. Similarly to the home agent node 24, the packet data serving node may perform the authentication, authorization and accounting functions in conjunction with, or with the assistance of, an authentication, authorization and accounting server, such as a RADIUS server.

McDONNELL BOEHNEN
HULBERT & BERGHOFF
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

09801545.051401

When the mobile node 10 initiates a communication session with the radio network node 16 by sending a call setup indication to the radio network node 16 across a radio communication link, the radio network node 16 initiates a registration process with the packet data serving node 18. Typically, the radio network node 16 is configured with a number of packet data serving nodes that may provide services to the mobile node 10. In the known prior art, the radio network node 16 has no status information for any of the packet data serving nodes that are configured to operates with the radio network node 16. Thus, when the radio network node 16 initiates the registration process for the mobile node 10, the radio network node 16 randomly selects a packet data serving node for the mobile node 10. In such a system, some of the packet data serving nodes available to the radio network node may be quickly overloaded while the other ones are rarely used. Further, if a number of consecutive packet data serving nodes to which the radio network node 16 sends registration requests are overloaded, such packet data serving nodes most likely reject registration requests from the radio network node 16, thus, resulting in service delays for the mobile node 10.

Therefore, some of the problems associated with the existing prior art mobile IP networks concern inefficient selection of packet data serving nodes by radio network nodes. For example, as mentioned in the proceeding paragraphs, when the radio network node 16 initiates a registration process for the mobile node 10, the radio network node 16 randomly selects the packet data serving node 18 to provide services to the mobile node 10.

Thus, there is a need for a system and method for an intelligent selection of packet data serving nodes in a mobile IP network.

McDONNELL BOEHNEN
HULBERT & BERGHOFF
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

SUMMARY OF THE INVENTION

The system and method for a packet data serving node selection in an IP network are developed.

An embodiment of a method for providing Internet Protocol communication services involves detecting a communication session associated with a client device, such as a mobile node, on a first network device, such as a radio node, and responsive to detecting the communication session, sending a first message including a registration request from the first network device to a second network device, such as a control network entity. When the second network device receives the registration request, the second network device determines a network address of a third network device arranged to provide network services to the client device. Responsive to determining the network address of the third network device, the second network device sends to the first network device a first response message including the network address of the third network device. When the third network device receives the first response message a communication session is established between the client network device and the third network device.

In one embodiment, when the second network device receives the registration request message, the second network device determines whether the client device is associated with at least one active communication session. If so, the second network device determines the last network device providing communication services to the client device. Responsive to determining the last network device, the second network device determines whether the last serving node is available to service the client device and whether it is associated with the first network device. If so, the second network device sends a network address of the last serving device to the first network device, and the last serving device continues providing communication services to the client device. If the last serving network device is not available to

McDONNELL BOEHNEN
HULBERT & BERGHOFF
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

10481564.061401

serve the client device, the second network device determines a new network device to provide communication services to the client device and sends a network address of the new network device to the first network device in a registration reply message. Further, the second network device sends an update message to the last serving network device to notify the last serving network device regarding the handoff of the client device to the new network device. Responsive to receiving the update message, the last serving node terminates any communication sessions associated with the client network device.

These as well as other aspects and advantages of the present invention will become more apparent to those of ordinary skill in the art by reading the following detailed description, with reference to the accompanying drawings.

09831549.051401

McDONNELL BOEHNEN
HULBERT & BERGHOFF
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

BRIEF DESCRIPTION OF THE DRAWINGS

Exemplary embodiments of the present invention are described with reference to the following drawings, in which:

Figure 1 is a block diagram illustrating an example of a prior art mobile IP network architecture;

Figure 2 is a block diagram illustrating an example of a mobile IP network architecture according to an embodiment of the present invention;

Figure 3 is a flow chart illustrating an exemplary method for foreign agent discovery process on a foreign agent control node according to one embodiment of the present invention;

Figure 4 is a message sequence scenario, according to one embodiment of the present invention, illustrating an exemplary message flow for discovering foreign agents on a foreign agent control node using heartbeat message;

Figure 5 is a block diagram illustrating an example of a heartbeat message format for messages sent from foreign agents to a foreign agent control node, according to one embodiment of the present invention;

Figure 6 is a block diagram illustrating an example of a heartbeat message format for messages sent from a foreign agent control node to foreign agents, according to one embodiment of the present invention;

Figure 7 is a flow chart illustrating a configuration of a radio network node according to one embodiment of the present invention;

Figures 8A and 8B are a flow chart illustrating a method for selecting a foreign agent on a foreign agent control node according to one embodiment of the present invention;

McDONNELL BOEHNEN
HULBERT & BERGHOFF
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

09834540.051401

Figure 9 is a message sequence scenario illustrating an example of a message flow for selecting a foreign agent on a foreign agent control node according to one embodiment of the present invention;

Figures 10A, 10B and 10C are a flow chart illustrating an example of a method for authenticating a mobile node associated with a foreign agent according to one embodiment of the present invention;

Figure 11 is a message sequence scenario illustrating an example of a message flow for a first time mobile Internet Protocol registration of a mobile node with a foreign agent selected on a control node;

Figure 12 is a message sequence scenario illustrating an example of a message flow for a first time simple Internet Protocol registration of a mobile node with a foreign agent selected on a control node; and

Figure 13 is a message sequence scenario illustrating a mobile node handoff between foreign agents.

10983156.061401

McDONNELL BOEHNEN
HULBERT & BERGHOFF
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

THE DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT(S)

Figure 2 is a functional block diagram illustrating an embodiment of a preferred network architecture suitable for application in the present invention for selecting foreign agents for mobile nodes in a mobile IP network. Figure 2 describes network entities typically employed in third generation mobile IP networks; however, it should be understood that the present invention is not limited to the network architecture described hereinafter, and the methods and apparatus described herein may be applied for managing the selection of foreign agents in any existing or later developed mobile IP systems. Referring to Figure 2, a client device, such as a mobile node 210, communicates with a remote client device, such as the target host 34, on the IP network 30. The mobile node 210 is connected to a first network device, such as a radio node 216, via a radio connection 238 on a radio access network. In one embodiment, the radio node may include a radio network node ("RNN"), a base station control ("BSC") node or a Packet Control Node ("PCN"), for example. As illustrated in Figure 1, the radio node is referred hereinafter as a radio network node. According to one embodiment of the present invention, the radio network node 216 communicates with a second network device, a foreign agent control node ("FACN") 220 and a plurality of packet data serving nodes ("PDSNs"). The FACN 220 manages foreign agents selection, such as a packet data serving node selection for mobile IP registration purposes. The FACN 220 may be referred to herein as a "control node", a "foreign agent control node", and the PDSNs may be referred herein as "foreign agents".

The FACN 220 includes a radio node mobile IP interface 224 for communicating with radio network nodes, such as the radio network node 216. When the radio network node 216 detects a call set up request from the mobile node 210, the radio network node 216 requests mobile registration service from the FACN 220 over the radio network node interface 224. When the FACN 220 receives a registration request, the FACN 220 selects a third network

McDONNELL BOEHNEN
HULBERT & BERGHOFF
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

device to provide network services to the mobile node 210. In one embodiment, the FACN 220 selects a PDSN using a set of predetermined criteria and sends the selected PDSN network address to the radio network node 216. The FACN 220 further includes a PDSN interface 230 for communicating with the pool of PDSNs, such as the PDSNs 232, 234, and 236. In the embodiment illustrated in Figure 2, the FACN 220 communicates via the PDSN interface 230 with FACN-managed PDSNs 232, 234, and 236. The PDSNs 232, 234, and 236 provide their capacity information capabilities, such as current call load factors, processing unit load factors, or memory load factors, via the PDSN interface 230.

In one specific embodiment, the PDSN interface 230 and the RNN interface 224 may be implemented in a Total Control Enterprise Network Hub commercially available from 3Com Corporation of Santa Clara, California. The Total Control product includes multiple network interface cards connected by a common bus. See "Modem Input/Output Processing Signaling Techniques," U.S. Patent No. 5,528,595, granted to Dale M. Walsh et al. for a description of the architecture of the Total Control product, which is incorporated herein by reference herein. However, the interfaces may also be implemented in other devices with other hardware and software configurations and are not limited to implementations in a Total Control product or the equivalent.

In one embodiment, the FACN 220 uses the capacity information of the managed PDSNs to determine the ability of a PDSN to handle a new mobile nodes registration. When the radio network node 216 registers the mobile node 210 with the FACN 220, the FACN 220 may first attempt to assign the registering mobile node 210 to the PDSN currently providing communication services to the mobile node. However, if the FACN has no active history for the mobile node 210, or if the PDSN currently serving the mobile node 210 is unavailable or invalid

McDONNELL BOEHNEN
HULBERT & BERGHOFF
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

for the radio network node 216, a new PDSN is selected from a PDSN pool associated with the registering radio network node 216.

Referring back to Figure 2, the FACN 220 further includes a memory unit 226. The memory unit 226 includes a volatile memory unit 226A and a nonvolatile memory unit 226B. In one embodiment, before the FACN 220 initiates processing of radio network node registration requests, the FACN 220 is configured with a number of configuration records or tables that may be stored in the nonvolatile memory unit 226B or, alternatively, may be stored to a configuration file by a system administrator. In an embodiment where the nonvolatile records are stored in the configuration file, any subsequent FACN startups may restore the configuration file. The configuration of the FACN 220 may be done via a Command Line Interface ("CLI") or a Simple Network Management Protocol ("SNMP") interface 228. The CLI/SNMP interface 228 provides a manner in which to add, delete and modify configuration entries. Any type of interface that provides an access for configuration may be used as an alternative to the interface 226. In one embodiment, a hardware platform for the FACN 220 may include a Sun Microsystems Netra hardware platform. However, different hardware platform

One of the configuration tables in the nonvolatile memory 226B may include port numbers for exchanging control data between the FACN 220, the PDSNs 232, 234, 236 and the radio network node 216. For example, the FACN 220 may employ User Datagram Protocol ("UDP") ports for exchanging control data with the PDSNs and the radio network node 216. The FACN 220 may be configured to use an UDP port number 697 for exchanging data with the radio network node 216. The FACN 220 may further be configured to use default UDP ports 15000 and 15001 for communicating control data with the PDSNs. However, it should be understood that the present invention is not limited to using these port numbers, and the FACN

McDONNELL BOEHNEN
HULBERT & BERGHOFF
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

220 may employ different ports for communicating control data with the radio network node and PDSNs.

The secure communication between network entities in communication systems often requires a receiving network entity to authenticate a sending entity. One example of secure communication between network entities involves the use of digital keys that are shared by communicating network entities. In such an embodiment, when a sending entity transmits a message to a receiving entity, the sending entity runs the message through a message digest algorithm using a secret key shared between the sending entity and the receiving entity, and produces a value commonly referred to as a message digest. The message digest is sent from the sending entity along with the message to the receiving entity that uses the message digest to verify whether the sending entity is a trusted entity. To do that, the receiving entity may extract the message digest from the received message and run the message through the same message digest algorithm. In such an embodiment, if the message digest generated on the receiving entity matches the one extracted from the received message, then, the user is a trusted entity. The process for authenticating entities is further described in the RFC-2002. However, the embodiments described herein are not limited to using the digital keys, and different or equivalent authentication methods may alternatively be used.

Referring again to Figure 2, the nonvolatile memory unit 226B preferably stores a number of digital secret keys. As mentioned in the preceding paragraphs, the PDSNs may authenticate the mobile node 210 with the assistance of an authentication, authorization and accounting ("AAA") server 240. Thus, one of the keys may include an AAA-PDSN secret key that is used on a PDSN and the AAA server, such as, for example, access-request or access-accept messages, to authenticate messages that are exchanged between the two entities during the authentication process. The AAA server 240 may be a Steel Belted RADIUS, Advanced

McDONNELL BOEHNEN
HULBERT & BERGHOFF
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

Wireless Edition ("SBR-AWE") provided by a service provider "FUNK", for example. In one embodiment, the FACN 220 may store a single AAA-PDSN secret key for the use between the AAA server and the PDSNs associated with the FACN 220. However, more than one secret key could also be used, so that, for example, predetermined sets of PDSNs are associated with different secret keys for communicating with one or more AAA servers. For example, an AAA-PDSN secret key record may include a secret key stored with an IP address of an AAA server assigned to the key. Table 1 illustrates an exemplary FAAA-PDSN secret key record.

AAA IP ADDRESS	SECRET KEY
IP address of an AAA	Secret key for the IP address

Table 1.

Similarly, the nonvolatile memory unit 226B may store FACN-PDSN and radio network node-PDSN secret keys. In one embodiment, one global secret key may be defined for the use between the FACN 220 and all PDSNs associated with the FACN 220. Table 2 illustrates an exemplary FACN-PDSN secret key record.

SECURITY PARAMETER INDEX	SECRET KEY
Security Parameter Index	Secret key for PDSN/FACN

Table 2.

Similarly, the radio network node 216 and the PDSNs may use the same secret key. Table 3 illustrates an exemplary radio network node -PDSN secret key record.

SECURITY PARAMETER INDEX	SECRET KEY
Security Parameter Index	Secret key for PDSN/radio network node

Table 3.

Further, according to one embodiment, a system operator of the FACN 220 may group a number of PDSN IP addresses that the FACN 220 will service and may assign a text description to each group so that each PDSN managed on the FACN 220 is assigned to at least one group. However, the present invention is not limited to grouping PDSNs by system operators, and

McDONNELL BOEHNEN
HULBERT & BERGHOFF
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

PDSNs may be automatically grouped to one or more groups, such as default groups, upon reporting to the FACN 220, as will be described in detail below. Table 4 illustrates an example of a record for grouping PDSNs, where an IP address of a PDSN specified by the system operator is assigned to a predetermined group number or a group identifier.

PDSN GROUP #	PDSN GROUP DESCRIPTION	PDSN IP ADDRESS LIST
Group number/Group ID	Group description	PDSN IP ADDRESS

Table 4.

Further, upon an initial FACN startup, the operator has the option of configuring a set of radio network node IP addresses that the FACN 220 will service. In one embodiment, a radio network node record may define a list of PDSN groups that may be selected to service radio network node requests. For example, if the operator fails to assign at least one PDSN group to a radio network node, the radio network node may be assigned to a default PDSN group when it attempts to register with the FACN 220 for the first time. Table 5 illustrates an exemplary radio network node-PDSN group assignment record in the nonvolatile memory unit 226B, where a radio network node IP address is assigned to one or more PDSN groups.

RADIO NETWORK NODE IP ADDRESS	PDSN GROUP LIST
IP address of an radio network node	A list of PDSN group numbers/Group Ids for the radio network node

Table 5.

Further, the FACN 220 may keep a number of volatile records that are created during the operational stage of the FACN 220. For example, such records may be stored on the volatile memory unit 226A. The FACN 220 may maintain volatile PDSN profile records and volatile mobile node records. The FACN 220 creates PDSN profile records as the PDSNs report their presence in the network. The PDSN profile records are dynamically changed as PDSNs become inactive or as new PDSNs are added to the network. According to an embodiment of the present invention, PDSNs are arranged to provide their load status information via periodic messages,

McDONNELL BOEHNEN
HULBERT & BERGHOFF
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

hereinafter referred to as heartbeat messages. Each PDSNs is configured to periodically send, for example, its processing load factor, call load factor, and/or memory load factor to the FACN 220. For example, the processing load factor of a PDSN may be associated with the processing capacity of the PDSN, the call load factor may be associated with a number of calls that the PDSN is currently serving, and the memory load factor may be associated with memory resources, either available or used, on the PDSN. According to one embodiment of the present invention, the FACN 220 is configured via the CLI/SNMP interface 226 with a number of threshold levels defining when a PDSN is no longer available for selection. For example, a call balance threshold may define a call level below which the PDSN may be selected to service new calls, independently of any call balancing mechanisms. In one embodiment, the FACN 220 may be automatically configured with a number of default threshold levels, such as, for example, 100% processing load, 100% memory load, and 4000 calls load level. In one embodiment, the FACN 220 may be configured with a number of thresholds that vary among the various PDSNs.

If a PDSN fails to send a heartbeat message for a predetermined number of consequtive periods, the FACN 220 may identify such a PDSN as unavailable. Like the other threshold, this number is preferably configurable in the PDSN entries as a "missed heartbeat count" variable. Further, each PDSN profile record may include a lifetime timer defining a time interval within which the FACN 220 should expect the consecutive heartbeat message. Table 6 illustrates an example of a PDSN profile record that may be created on the FACN 220 for each PDSN during the operational stage of the FACN 220.

PDSN	STATUS	MISSED HEARTBEAT COUNT	LIFETIME TIMER	LOAD FACTOR
PDSN IP address	Inactive/Active	Number of missed heartbeat messages	Heartbeat message timer	Processing/ Memory/ Call Loading

Table 6.

McDONNELL BOEHNEN
HULBERT & BERGHOFF
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

Further, the FACN 220 may maintain mobile user information data in mobile node records that are created on the FACN 220 upon user registrations with a FACN-managed PDSN. Each time a mobile node registers with one of the FACN-managed PDSNs, the registering PDSN may send the mobile node's data, such as an AAA profile and mobile session information, to the FACN 220, so that if no record currently exists for the mobile node, the FACN 220 may create a new mobile user profile record, or if such a record already exists, the FACN 220 may update the currently existing record associated with the mobile user. Further, if such a record already exists, but for a different PDSN than the one sending the update, then, a "PDSN handoff" has occurred, that is, the mobile node has roamed from one radio node to a new radio node that is not associated with the original serving PDSN, or that the original PDSN is unavailable for some other reasons, such as, its call load is excessive or it is no longer sending heartbeat messages, for example. According to one embodiment, when the FACN 220 detects the handoff, the FACN 220 may send an update message to the previous PDSN associated with the AAA profile and mobile session information. Upon the receipt of this message, the previous PDSN may terminate its communication link with the previous radio node associated with the mobile node.

A mobile user profile record may include a mobile telephone number or an International Mobile Subscriber Identity ("IMSI"), a mobile connection identifier ("MOBILE NODE-ID"), one or more sessions indexed by a Network Address Identifier ("NAI"), or a NAI user profile. Table 7 illustrates an exemplary mobile node profile record that may be created on the FACN 220 upon receiving registration information from a PDSN as the mobile node registers with the PDSN.

IMSI/MOBILE NODE-ID	MOBILE SESSION NAI	PDSN IP ADDRESS	MOBILE SESSION STATUS	MOBILE PROFILE
Mobile phone number and connection ID	Mobile session NAI (user@domain)	IP address of the last PDSN	Active or idle	AAA profile of the mobile session

McDONNELL BOEHNEN
HULBERT & BERGHOFF
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

Table 7.

It should be understood that the present invention is not limited to the use within the system illustrated in Figure 2. More, fewer or different components, connections, interfaces could also be used. For example, the volatile and nonvolatile records described in the preceding paragraphs may be stored in one or more databases located on the FACN 220 or may be stored on a volatile or nonvolatile media in a network server in communication with the FACN 220. Additionally, the radio node is not limited to the radio network node, and different types of radio nodes could also be used, such as a Base Station Controller ("BSC") node or a Packet Control Function ("PCF") node, for example. Further, the arrangements described herein are shown for purposes of illustration only, and those skilled in the art will appreciate that other arrangements and other elements, such as interfaces or functions, whether or not known in the art, can be used instead, and some elements may be omitted altogether. Additionally, as in most communications applications, those skilled in the art will appreciate that many of the elements described herein are functional entities that may be implemented as discrete components or in conjunction with other components, or as firmware or software, in any suitable combination and location.

Figure 3 is a flow chart illustrating a method 300 for a foreign agent discovery process, such as a PDSN discovery process. According to one embodiment, the foreign agent discovery process is implemented using a network protocol between the foreign agents and a control node, such as the FACN 220. When the foreign agent starts operating, the foreign agent sends an initialization control message to the control node, thus, conveying its ability to handle mobile node registration requests. Referring to Figure 3, at step 302, a control node receives an initialization control message from a foreign agent. Responsive to receiving the initialization control message, the control node generates an initialization control reply message including secret key data. For example, the secret key data may include a first secret key that may be used

McDONNELL BOEHNEN
HULBERT & BERGHOFF
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

09841507.021401

when the foreign agent communicates with a radio network node, and a second secret key is used when the foreign agent communicates with a predetermined AAA network server. At step 304, the control node sends the initialization control reply message to the foreign agent. Further, at step 306, the control node dynamically creates a foreign agent profile record and marks the foreign agent as an inactive foreign agent. In one embodiment, the dynamic foreign agent profile entry may be stored in a memory configured to store volatile records. However, different embodiments are possible as well. For example, the control node may be configured to store the volatile records in one or more databases.

Responsive to receiving the initialization control reply message from the control node, the foreign agent may start its normal operation of sending periodic control messages to the control node. According to an exemplary embodiment, the control messages that are periodically sent from the foreign agent indicate that the foreign agent is active and include load data associated with the foreign agent, such a call load factor, processing load factor, and/or memory load factor associated with the call, processing and memory resources that are currently used by the foreign agent. At step 308, the control node determines whether a second control message has been received from the foreign agent. If the second message is not received, the method 300 terminates, and the foreign agent's inactive status in the foreign agent profile record is not changed. If the second control message is received by the control node, at step 310, the control node modifies the foreign agent's inactive status in the foreign agent's record to an active status. Further, if the second control message includes load factors associated with the foreign agent, at step 312, the control node stores the load factors in the foreign agent profile record. Further, the control node may send a reply acknowledgement message to the control node, thus, indicating its active state and the receipt of the second message.

McDONNELL BOEHNEN
HULBERT & BERGHOFF
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

In the method 300, the control node may be the FACN 220, described above, and the foreign agent may be the PDSN 232. However, it should be understood that the method 300 is not limited to the use of any particular hardware or software and fewer, more, different or equivalent network devices may also be used.

According to an exemplary embodiment, the control node, FACN 220, and the associated foreign agents, PDSNs, may use a heartbeat messaging mechanism to convey the foreign agent availability, control node availability and foreign agent load factors. Figure 4 is an example of a message sequence scenario 400 illustrating a heartbeat-messaging scheme that may be used between a foreign agent and a control node. A foreign agent, such as the PDSN 232, starts communication with a control node, such as the FACN 220, via a Heartbeat Initialization ("INIT") message 402. Responsive to receipt of the Heartbeat INIT message 402, the control node generates a Heartbeat INIT Acknowledge message 404, including secret keys to be used on the foreign agent for communication with the radio network node 216 and a predetermined AAA server, and transmits the message 404 to the foreign agent. Subsequently, the foreign agent sends to the control node periodic Heartbeat messages 406 including its processing, memory and call load factors, or a status override parameter indicating that the foreign agent is unavailable. In accordance with a preferred embodiment, the heartbeat messages are periodic in nature. The control node responds to each periodic heartbeat message with a Heartbeat Acknowledge message 408. In one embodiment, the Heartbeat Acknowledge message 408 may include a unique key tag identifier associated with the AAA server and radio network node keys. The control node may update keys available to the foreign agent, and if one or more keys are updated, the control node may define a new key tag identifier in a Heartbeat Acknowledge message. If the foreign agent receives a new key tag identifier, the foreign agent may request new keys via a Heartbeat INIT message.

McDONNELL BOEHNEN
HULBERT & BERGHOFF
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

10045715.050401

According to one embodiment, the periodic Heartbeat messages are indicative of the foreign agent's activity and include foreign agent's load factors. As mentioned in reference to the preceding paragraphs, the control node may be configured to remove a foreign agent from a list of active foreign agents if a predetermined number of periodic heartbeat messages are missing or if a predetermined number of periodic heartbeat messages fails authentication on the control node. According to another embodiment, heartbeat messages, such as a Heartbeat INIT and periodic Heartbeat messages, may include heartbeat intervals so that the control node expects to receive the next heartbeat message from the foreign agent prior to an end of the heartbeat interval specified by the foreign agent in the previous heartbeat message.

Figure 5 is a block diagram illustrating a preferred format 500 of heartbeat messages, such as preferred formats of the Heartbeat INIT message 402 and the periodic Heartbeat messages 406. The message format 500 includes a plurality of fields: an IP header 502, an UDP header 504, a message type field 506, a reserved field 508, a length field 510, a heartbeat interval field 512, a reserved field 514, a PDSN address field 516, and a plurality of sub-fields. The IP header 502 may have a format of an IP header. In such an embodiment, a destination field in the IP header may include an IP address of the control node and a source address field may include an IP address of a source foreign agent, such as the PDSN 232 of Figure 2. However, the IP header is not limited to the IP header, and different IP header formats could also be used. Further, in one embodiment, the UDP header format 504 may have a format of the UDP header, for instance. Alternative formats for the heartbeat messages may also be used. For example, the heartbeat messages may include more or fewer fields and/or subfields than are shown in Figure 5, or arrangement of the fields and/or subfields may be changed.

McDONNELL BOEHNEN
HULBERT & BERGHOFF
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

The type field 506 defines a type of the Heartbeat message, such as a PDSN INIT Heartbeat or a PDSN periodic Heartbeat. Table 8 illustrates an example of message type values for the two messages. Other type values may alternatively be used.

TYPE	DETAILS
0x02	PDSN INIT Heartbeat
0x01	PDSN periodic Heartbeat

Table 8.

Further, the reserved fields 508 and 514 may be left blank for a future use or, alternatively, eliminated. The length field 510 may define a message length, for example, in octets, and the heartbeat interval 512 may define a time interval during which time the control node should receive the next heartbeat message. The foreign agent address field 516 includes, for example, an IP address of the foreign agent sending the message.

The plurality of sub-fields includes load factors of the sending foreign agent. In the message format illustrated in Figure 5, there are three subtype load fields: a call load field 518, a processing usage field 524, and a memory usage field 536, with the respective length fields 520, 526, and 538, and value fields 522, 528, and 534 defining the current load factors of the variables defined in the fields 518, 524, and 536. Table 9 illustrates exemplary values that may be used for the subtype fields 518, 524, and 536. However, it should be understood that different values for the call load, processing usage, and the memory usage fields could also be used. Further, fewer, more, different or equivalent foreign agent capacity variables could also be used.

SUBTYPE	DETAILS
0x12	Foreign Agent Call Load
0x52	Foreign Agent CPU Usage
0x32	Foreign Agent Memory Usage

Table 9.

Further, the message format of Figure 5 includes an authentication type field 536 with an identifier of an authentication mode employed on the foreign agent, a length field 538 including

McDONNELL BOEHNEN
HULBERT & BERGHOFF
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

a length of the authentication field 536, a Security Parameter Index ("SPI") fields 540, 542 and an Authenticator field 544.

Figure 6 illustrates an example of a message format 600 for heartbeat messages that may be sent from the control node in response to receiving a heartbeat message from a foreign agent, such as the FACN Heartbeat INIT ACK message 404 or the FACN periodic Heartbeat ACK message 408 illustrated in Figure 4. The message format illustrated in Figure 6 is similar to the one shown in Figure 5, and includes an IP header field 602, an UDP header field 604, a message type field 606, a reserved field 608, a length field 610, and a PDSN address field 612. Like the message format 500 in Figure 5, the message format 600 is merely an example of a preferred embodiment and alternative formats may be used. For example, the heartbeat messages may include more or fewer fields and/or subfields that are shown in Figure 6, or the arrangement of fields and/or subfields may be changed.

In Figure 6, the IP header field 602 includes a source address field with an IP address of the FACN 220, and a destination address field with an IP address of a destination PDSN. Further, the message type field identifies a type of the heartbeat message that is generated by the FACN 220. Table 10 illustrates an example of type values that may be used to define a heartbeat INIT ACK message and periodic ACK message type.

TYPE	DETAILS
0x12	Heartbeat INIT ACK from FACN
0x11	Periodic Heartbeat ACK from FACN

Table 10.

The message format 600 also includes a key tag value field 614, a reserved field 616, a subtype PDSN-radio network node key field 618, a length field 620 associated with the subtype key field, an SPI field 622, and secret fields 624. The key tag value field 614 includes a sequential key tag identifier for the AAA and radio network node keys stored on the FACN 220. The sequential key tag identifiers may be modified on the FACN 220 each time one or both

McDONNELL BOEHNEN
HULBERT & BERGHOFF
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

keys are changed. If a PDSN receiving a heartbeat ACK message from the FACN 220 detects that a key tag identifier specified in the received message is different from a key tag identifier stored locally on the PDSN, the PDSN may send a Heartbeat INIT message to cause the FACN 220 to refresh its keys. The subtype PDSN-radio network node key field 618 identifies the type of a secret key in the secret fields 624. According to the embodiment illustrated in Figure 6, the subtype PDSN-radio network node key field 618 includes an identifier associated with the PDSN-radio network node key that is included in the secret key fields 624.

Further, the message includes a subtype PDSN-AAA key field 626, a length field 628, an AAA IP address field 630, secret fields 632, an authentication type field 634, a length field 636, an SPI field 638, and an SPI authenticator field 640. The subtype PDSN-AAA key field 626 identifies that the secret fields 632 include an AAA key that may be used between the PDSN and an AAA server. In one embodiment, a network address, such as an IP address, of the AAA server is specified in the AAA IP address field 630. [What is defined in the authentication type, SPI and SPI authenticator fields?] Table 11 illustrates exemplary type values that may be used in the subtype fields 618 and 626. However, different values could also be used.

SUBTYPE	DETAILS
0x41	PDSN-radio network node key
0x51	PDSN-AAA key

Table 11.

Figure 7 is a flow chart illustrating a method 700, in accordance with a preferred embodiment, for a radio network node operation. At step 702, a radio network node is configured with a network address of a control node as a preferred foreign agent network address. In such an embodiment, when the radio network node detects a mobile node in its service area, the radio network node queries the control node prior to attempting to register the mobile node with any other foreign agent. The radio network node may be configured with a number of network addresses of foreign agents available to serve mobile nodes in the service

McDONNELL BOEHNEN
HULBERT & BERGHOFF
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

area of the radio network node. At step 704, the radio network node determines whether a new mobile node has been detected in its service area. If the radio network node detects a new mobile node in its service area, then, at step 706, the radio network node sends a registration request to the network address of the control node. Otherwise, the method returns to step 704.

At step 708, the radio network node receives a registration reply message from the control node. According to a preferred embodiment, the registration reply message includes a network address of a foreign agent selected on the control node. Such selection may be based on a number of the selection criteria described in reference to Figure 8A and 8B. Alternatively, the registration reply message may include a rejection code if the radio network node fails an authentication process on the control node, for instance. In such an embodiment, the radio network node may send a registration request message to one of the foreign agents with which the radio network node is configured.

At step 710, the radio network node sends a registration request message to the foreign agent node specified in the registration reply message from the control node. The registration request message may include the mobile node's data, such as, for example, a mobile identifier or a network address of a home agent associated with the mobile node. At step 712, the radio network node receives a registration reply message from the foreign agent. The registration reply message received on the radio network node may include a registration confirmation parameter or a registration rejection parameter. If the registration reply message includes the registration confirmation parameter, the mobile node may initiate establishing of a communication link, such as a point-to-point communication link, with the foreign agent. If the registration reply message includes the registration rejection parameter, the radio network node may retry to register with the foreign agent control node or, alternatively, may register with another foreign agent with which it was configured.

McDONNELL BOEHNEN
HULBERT & BERGHOFF
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

In the method 700 described in reference to Figure 7, the mobile node may include the mobile node 210, the radio network node may include the radio network node 216, the foreign agent control node may include the FACN 220, and the foreign agent may include the PDSN 232, as illustrated in Figure 2. However, the exemplary method is not limited to these devices, and fewer, more, or different devices may alternatively be used so long as such devices are capable of performing the steps recited in Figure 7.

As mentioned in the preceding paragraphs, one of the control node's functions is to select a foreign agent to service the radio network node's mobile client registration requests. When the control node receives a registration request message from the radio network node 216, the control node does not process the registration request as a typical foreign agent normally does. Instead, it selects a foreign agent, such as one of the PDSNs 232, 234, or 236 illustrated in Figure 2 that can service the mobile client registration. The control node may use any appropriate selection algorithm to determine a foreign agent that is suitable to service a mobile client registration.

Figures 8A and 8B are a flow chart illustrating a method 800 that may be controlled on a control node for selecting a foreign agent to service a mobile client's registration request. At step 802, the control node receives a registration request message from a radio network node responsive to detecting a mobile node in a service area of the radio network node. The registration request message includes the mobile node's information, such as mobile node's home agent data, the radio network node's data, and a request for the mobile node's registration. In one embodiment, the registration request message may have a message format described in the RFC 2002; however, different message formats may alternatively be used.

At step 804, the control node authenticates the radio network node upon receipt of the registration request message. Upon a successful authentication of the radio network node, then,

McDONNELL BOEHNEN
HULBERT & BERGHOFF
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

at step 806, the control node determines whether at least one session associated with the mobile node is active. To do that, the control node may determine whether user information associated with the mobile node is available on the control node. In one embodiment, the control node may retrieve its mobile user information records to determine whether such a record exists for the mobile user specified in the registration request message. In one embodiment, the mobile user information records include, among other parameters described in reference to Table 7, foreign agent-mobile user binding information. According to a preferred embodiment, the foreign agent-mobile user information is updated on the control node each time the mobile node is assigned to a new foreign agent. Thus, if the mobile node's status is active, the foreign agent in the record corresponds to the foreign agent that is currently serving the mobile node.

In one embodiment, if the control node has the mobile user information record available, the control node attempts to first select the foreign agent that is currently serving the mobile node. At step 808, the control node determines a foreign agent associated with the mobile node using the mobile user information record. At step 810, the control node determines whether the foreign agent associated with the mobile node is available to service the mobile node registration request. To do that, the control node may invoke an information record associated with the foreign agent to determine load factors of the foreign agent. According to one embodiment, the load factors may include a memory load factor, a processing load factor and a call load factor associated with the foreign agent. The control node may be configured with threshold levels for each of the load factors defining maximum limits for the memory usage, processing usage or call load on the foreign agent. The control node may then verify the availability of the foreign agent by determining whether the load factors of the foreign agent do not exceed the threshold levels.

If the foreign agent is available to service the registration requests of the mobile node, then, at step 812, the control node determines whether the particular foreign agent, determined at

McDONNELL BOEHNEN
HULBERT & BERGHOFF
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

step 808, is a valid foreign agent for the radio network node. To do that, the control node retrieves a radio network node information record that defines a group of foreign agents associated with the radio network node. If the evaluated foreign agent is one of the valid foreign agents for the radio network node, then, at step 814, the control node generates a registration reply message including a network address, such as an IP address, of the foreign agent selected to service the radio network node request.

However, if the control node determines that the mobile client is inactive (step 806), or that the foreign agent is not available (step 810), or not valid for the radio network node, then the control node applies a search selection algorithm to determine a foreign agent that may serve the radio network node request. According to a preferred embodiment, the control node applies the search selection algorithm to one or more foreign agent groups associated with the radio network node. The foreign agent configuration for each radio network node may be done, for example, based on a number of specific criteria, which may include, for example, a geographic proximity between the radio network node and foreign agents, directional requirements (i.e. east to west), or a shortest network path between the radio network node and the foreign agent. In one embodiment, the radio network node may be associated with a number of foreign agent groups, and each group may include a number of foreign agents. In such an embodiment, the search selection algorithm for selecting a foreign agent to serve the radio network node request may be applied, in a defined order, to each foreign agent group associated with the radio network node and to search, in the defined order, each foreign agent within each examined foreign agent group. According to an exemplary embodiment, the search selection algorithm that is used to evaluate the foreign agent load factors initially loads foreign agents up to a configured call balanced threshold, and then uses a load balancing to determine a foreign agent, as described in greater detail below.

McDONNELL BOEHNEN
HULBERT & BERGHOFF
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

Thus, if the control node determines that the mobile client is inactive (step 806), the foreign agent is not available (step 810), or not valid for the registering radio network node (step 812), then, the method 800 continues at step 816, where the control node determines at least one foreign agent group associated with the radio network node. At step 818, the control node determines whether the foreign agents in each group has been front loaded up to a predetermined call balance threshold. If the control node determines that at least one foreign agent has a call load lower than the predetermined call balance threshold, the control node preferably selects the first such foreign agent to service the registration request of the radio network node. At step 820, the control node generates a registration reply message including a network address, such as an IP address, of the foreign agent that has the call load lower than the call balance threshold.

If all foreign agents associated with the foreign agent groups of the radio network node have been already front-loaded up to, for example, a predetermined call balanced threshold load, the control node applies a load balancing scheme to select a foreign agent for the radio network node. However, it should be understood that the present invention is not limited to front-loading the foreign agents up to the predetermined call balanced threshold load, and different embodiments are possible as well. The load-balancing scheme may be based on load factors of the foreign agents associated with the radio network node. At step 822, the control node applies a load-balancing method to determine a foreign agent to service the registration request of the radio network node. The control node determines the foreign agent using the load factors associated with each foreign agent. In one embodiment, the control node may select a foreign agent that has the least number of calls, however, different embodiments are possible as well. For example, the foreign agent may be selected based on the highest processing capacity or the most memory availability. Alternative search selection algorithms may also be used. For, example, a foreign agent may be selected using a load balancing technique, but without front-

McDONNELL BOEHNEN
HULBERT & BERGHOFF
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

loading. As a further example, the search selection algorithm may be applied to foreign agents without regard to any defined order. These and other alternatives will be apparent to those skilled in the art upon reading this detailed description.

At step 824, the control node generates and sends a registration reply message to the radio network node. The registration reply message includes a network address, such as an IP address, of the foreign agent determined using the load-balancing method.

In the method 800 described with reference to Figures 8A and 8B, the mobile node may include the mobile node 210, the radio network node may include the radio network node 216, the foreign agent control node may include the FACN 220, and the foreign agent may include the PDSN 232, 234 or 236 as illustrated in Figure 2. However, the method 800 is not limited to these devices, and fewer, more, or different devices may alternatively be used as long as such devices are operable to perform the steps shown in Figures 8A and 8B.

Figure 9 is a block diagram of a message sequence scenario 900 illustrating a foreign agent selection method. The block diagram includes the mobile node 210, the radio network node 216, the FACN 220 and the PDSN 232, as illustrated in Figure 2. When the mobile node 210 roams into a service area of the radio network node 216, the mobile node 210 sends a service origination ("SO") message 902 to the radio network node 216, and the radio network node 216 responds with a base origination ("BS") acknowledge order message 904. Upon receiving the BS acknowledge message 904 at the mobile node 210, the mobile node 210 and the radio network node 216 set up a communication link such as a tunnel communication link illustrated by reference number 906.

Upon establishing the communication link between the mobile node 210 and the radio network node 216, the radio network node 216 sends a registration request message 908 to the FACN 220. As illustrated in Figure 9, the registration request message 908 includes a lifetime

McDONNELL BOEHNEN
HULBERT & BERGHOFF
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

parameter defining a lifetime value associated with the message, and mobile node-home agent extensions defining user profile parameters, for example. When the FACN 220 receives the registration request message 908, the FACN 220 selects a PDSN for the mobile node 210 based, for example, on the load and/or processing factors, International Mobile Subscriber Identity and last serving PDSN mapping, as illustrated in block 910. When the FACN 220 selects a PDSN to service the registration request, the FACN 220 generates and sends to the radio network node 216 a registration reply message 912. According to one embodiment of the present invention, the FACN 220 does not provide foreign agent functionality and, instead, it selects PDSNs using a predetermined set of criteria, described in reference to Figures 8A and 8B. Thus, the registration reply message 912 includes a registration rejection code 136, for instance in which no suitable foreign agent is identified, or, further, includes a network address, such as an IP address, of the PDSN selected by the FACN 220 (in this example, the IP address of the PDSN 232).

When the radio network node 216 receives the registration reply message 912 including the network address of the selected PDSN, the radio network node 216 sends a registration request message 914 to the PDSN specified in the reply message. According to the embodiment illustrated in Figure 9, the radio network node 216 sends the registration request message 914 including a lifetime parameter and mobile node-home agent extensions to the PDSN 232. Upon an authentication of the mobile node 210 by the PDSN 232, the process of which will be described hereinafter, the PDSN 232 sends a registration reply message 916 to the radio network node 216. When the radio network node 216 receives the registration reply message 916 including a registration accept response from the PDSN 232, the mobile node 210 may establish a communication link, such as a point-to-point communication link, to the PDSN 232, as illustrated in 918. Upon establishing the communication link, the mobile node 210 registers with

McDONNELL BOEHNEN
HULBERT & BERGHOFF
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

the PDSN 232, and the mobile node 210 may start transmitting user data to a target host via the PDSN 232.

When the mobile node 210 establishes a communication link with the PDSN 232 and sends a registration request message 914 to the PDSN 232, the PDSN 232 is arranged to authenticate the request. According to an exemplary embodiment, the FACN 220 maintains database records, for example, as illustrated in Table 7, of mobile clients successfully authenticated in previous registrations. Each time a mobile client registers, and the mobile client is not cached in the FACN database, a PDSN with which the mobile client registers sends AAA profile information to the FACN 220. Further, according to one embodiment, if the mobile client is authenticated and has an active status, the FACN 220 may provide the cached AAA profile information to a PDSN serving the mobile node 210, allowing the PDSN to skip AAA authentication.

Figures 10A, 10B and 10C are a flow chart illustrating a method 1000 for mobile node first time registration with a foreign agent, according to one embodiment of the present invention. Referring to Figure 10A, when a radio network node detects a new mobile node and successfully registers with a foreign agent selected on a control node, at step 1002, a communication link is established between the mobile node and the foreign agent specified by the control node. For example, the mobile node may establish a point-to-point communication link with the foreign agent. At step 1004, the mobile node sends a registration request message to the foreign agent. According to an exemplary embodiment, the foreign agent stores visitor list records including a list of mobile sessions associated with mobile nodes that are serviced on the foreign agent. The mobile sessions in the visitor list records on the foreign agent are associated with mobile nodes that are serviced by the foreign agent and, thus, have been previously authenticated. At step 1006, the foreign agent determines whether a visitor list record exists for

10083159.011401

McDONNELL BOEHNEN
HULBERT & BERGHOFF
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

the registering mobile node. If the foreign agent has the mobile node in its local visitor list records, the method 1000 continues at step 1030, described in greater detail below. If the foreign agent control node does not have the mobile node in the visitor list records, then, at step 1008, the foreign agent sends a visitor list registration request message including an authentication data request to the control node.

When the control node receives the visitor list registration request message from the foreign agent, at step 1010, the control node determines whether the mobile node has already been authenticated, and, thus, whether the control node includes authentication data for the mobile node. To do that, the control node may retrieve a mobile user's record including data associated with the mobile node's user. Further, using the mobile user's database record, the control node may determine an activity state of the mobile node. In one embodiment, the control node determines whether the mobile node has an active session status. If the control node determines that the authentication data for the mobile node is not available, or that the mobile user session in the record is defined as inactive, the control node rejects the visitor list registration request, and, at step 1016, sends to the foreign agent a visitor list reply message including an authentication data rejection parameter.

When the foreign agent receives the reply message including the authentication data rejection parameter, the foreign agent may employ other means to authenticate the mobile node's client. According to one embodiment, at step 1018, the foreign agent queries an authentication network server to authenticate the mobile node. Next, at step 1020, the foreign agent determines whether the mobile node client has been successfully authenticated. If the mobile node has failed the authentication, the method 1000 terminates. If the authentication process for the mobile node is successful, then, at step 1022, the foreign agent sends to the control node a registration update message including authentication data of the mobile node. When the control

McDONNELL BOEHNEN
HULBERT & BERGHOFF
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

node receives the registration update message, at step 1024, the control node updates or creates a new mobile user's record with the received authentication data of the mobile node. It is possible for the control node to receive the registration update message including authentication data of the mobile node indicating a foreign agent that is different than the one that originally sent an original update message for the registering mobile node, thus, indicating the foreign agent handoff. At step 1026, the control node determines whether the foreign agent in the update message is the same foreign agent as previously authenticated. If the foreign agent is different, at step 1028, the control node sends a registration update message to the foreign agent previously serving the mobile node. When the previously serving foreign agent receives the registration update message from the control node indicating that the mobile node has registered with a new foreign agent, at step 1030, the previously serving foreign agent may terminate its communication link to the radio node that previously serviced the mobile node. The foreign agent handoff can occur for a variety of reasons, such as when a mobile node's roams to a radio node that is not defined to communicate with the previously serving foreign agent, or when the previously serving foreign agent has exceeded one of its load thresholds. The foreign agent handoff will be further described in Figure 13.

Referring back to step 1010, if the control node determines that the authentication data for the mobile node's user is available and the state of the mobile node specified in the mobile user's record is active, the control node returns the authentication data to the foreign agent, thus, allowing the foreign agent to skip the authentication process. In such an embodiment, at step 1012, the control node sends a visitor list registration reply message including authentication data associated with the mobile node to the foreign agent. At step 1014, the foreign agent receives the visitor list reply message from the control node.

McDONNELL BOEHNEN
HULBERT & BERGHOFF
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

When the foreign agent has authentication data for the mobile node, then, at step 1032, the foreign agent registers with a home agent of the mobile node. In one embodiment, the registration process with the home agent may include sending from the foreign agent to the home agent a registration request message, and receiving a registration reply message at the foreign agent from the home agent. When the foreign agent successfully registers with the home agent, then, at step 1034, the foreign agent sends to the mobile node a registration reply message. When the mobile node receives the registration reply message from the foreign agent, the mobile node may start communicating data to a target host via the foreign agent and the home agent.

In the method 1000 described in reference to Figures 10A, 10B and 10C, the mobile node may include the mobile node 210, the foreign agent control node may include the FACN 220, the home agent may include a home agent 24, the authentication server may include a RADIUS server, and the foreign agent may include the PDSN 232, 234 or 236 illustrated in Figure 2. However, the exemplary method is not limited to these devices, and fewer, more, or different devices may alternatively be used, provided such devices are operable to perform the steps of Figures 10A, 10B and 10C.

Figure 11 is a block diagram of a message sequence scenario 1100 illustrating a first time registration of a mobile node with a foreign agent selected by a control node to provide network services to the mobile node. The block diagram includes the mobile node 210, the radio network node 216, the FACN 220, the PDSN 232, the HA 24 and the AAA server 240, as illustrated in Figure 2. The exemplary message sequence scenario of Figure 11 shows an embodiment in which the mobile node 210 establishes a PPP communication link with the PDSN 232. When the FACN 220 selects the PDSN 232 to service the mobile node 210, the mobile node 210 negotiates a PPP communication link with the PDSN 232 and initiates an agent discovery process, as illustrated at 1104 and 1106, respectively. Upon establishing the PPP communication

McDONNELL BOEHNEN
HULBERT & BERGHOFF
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

link, the mobile node 210 sends a registration request message 1108 to the PDSN 232. According to a preferred embodiment, the registration request (lifetime) message 1108 may have a message format described in accordance with RFC 2002. However, different or equivalent message formats may alternatively be used.

When the PDSN 232 receives the registration request message 1108 and the PDSN 232 does not have the mobile node in its local visitor list, the PDSN 232 sends a visitor registration request message 1110 to the FACN 220 to determine whether the FACN 220 has authentication data of the mobile node. In one embodiment, the registration request message 1110 includes a number of extension fields defining, for example, session specific parameters, mobile node NAI parameters and authentication parameters. The session specific extensions include information related to the communication session between the mobile node 210 and the PDSN 232, the mobile node NAI extensions include information related to the user profile employed between the mobile node 210 and the PDSN 232, and the authentication extensions include an authenticator value that may be computed on the PDSN 232 using a PDSN-FACN secret key. It should be understood that more, fewer, or equivalent extension fields may alternatively be used.

When the FACN 220 receives the registration request message 1110, the FACN 220 determines whether it has stored authentication data for the mobile node 210. According to the embodiment illustrated in Figure 11, the FACN 220, as illustrated at block 1112, has no previous authentication status associated with the mobile node 210. Since the FACN 220 does not have the authentication data of the mobile node 210, the FACN 220 rejects the visitor list registration request and sends a visitor list registration reject reply message 1114 to the PDSN 232. The visitor list registration reject reply message 1114 may include a number of parameters informing the PDSN 232 about the status of its request. For example, if the authentication data of the mobile node 210 is available on the FACN 220, a visitor list registration reply message may

McDONNELL BOEHNEN
HULBERT & BERGHOFF
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

include an authentication data available parameter, and, if the authentication data request is denied on the FACN 220, the visitor list registration reply message may include a reason for not providing the authentication data to the PDSN 232. For example, the FACN 220 may specify a failure of the foreign agent authentication process parameter, a registration identification mismatch parameter, a poorly formed request parameter, or an authentication data not available parameter.

When the PDSN 232 receives the visitor list registration reject reply message 1114, the PDSN 232 queries the AAA network server 1102 for the required authentication data of the mobile node 210, as illustrated in 1116. Once the mobile node 210 is authenticated, the PDSN 232 registers with the home agent 24. In one embodiment, the registration process with the home agent 24 includes sending a registration request message 1118 from the PDSN 232 to the home agent 24 and receiving a registration reply accept message 1120 at the PDSN 232 from the home agent 24. Upon a successful registration with the home agent 24, the PDSN 232 sends a registration reply accept message 1122 to the mobile node 210, thus, completing the registration process for the mobile node 210.

According to one embodiment, once the mobile node 210 is authenticated and registered with the home agent 24, the PDSN 232 informs the FACN 220 of the visitor list update. To do that, the PDSN 232 sends a visitor list registration update message 1124, preferably including the AAA profile that was determined by the PDSN 232 using the AAA server 1102. In addition to the extension fields discussed in reference to the visitor list registration request message 1110, the visitor list registration update message 1124 has a number of extension fields including the AAA profile of the mobile node 210. In one embodiment, the extension fields may be two octets long.

McDONNELL BOEHNEN
HULBERT & BERGHOFF
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

When the FACN 220 receives the visitor list registration update message 1122 from the PDSN 232, the FACN 220 updates the mobile user record of the mobile node 210. Further, in response to receiving the message 1122, the FACN 220 sends to the PDSN 232 a visitor list registration acknowledgement message 1126, thus, terminating the message sequence scenario illustrated in Figure 11. Upon a successful registration of the mobile node 210, the mobile node 210 may start communicating data with a remote entity, as illustrated by a bi-directional packet data call-up block 1128.

The message sequence 1100 described in reference to Figure 11 relates to the mobile IP first time registration process. However, the preferred embodiments are not limited to mobile IP, and are equally applicable when the mobile node 210 establishes simple IP sessions. Figure 12 is a block diagram of a message sequence scenario 1200 illustrating a first time simple IP registration with a foreign agent that is selected by a control node. The block diagram includes the mobile node 210, the radio network node 216, the FACN 220, the PDSN 232, and the AAA server 240, as illustrated in Figure 2. When the FACN 220 selects the PDSN 232 to service the mobile node 210, and the radio network node 216 registers with the PDSN 232, as described with reference to Figure 9, the mobile node 210 establishes a communication link with the PDSN 232. According to the embodiment illustrated in Figure 12, the mobile node 210 establishes a communication link with the PDSN 232 using a Link Control Protocol ("LCP") negotiation method 1204. Further, the mobile node 210 may send an access request message, such as a Password Authentication Protocol ("PAP")/ Challenge Handshake Authentication Protocol ("CHAP") request message 1206 to the PDSN 232. The PAP/CHAP request message 1206 includes a registration request and information data associated with the mobile node 210. When the PDSN 232 receives the PAP/CHAP request message 1206 and does not have the mobile node 210 in its local visitor list, the PDSN 220 sends a visitor list registration request message 1208 to

McDONNELL BOEHNEN
HULBERT & BERGHOFF
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

the FACN 232 to determine whether the FACN 232 has authentication data of the mobile node 210. The visitor list registration request message 1208 preferably includes a number of extension fields including session specific parameters, mobile node NAI parameters and authentication parameters of the PDSN 232.

When the FACN 220 receives the visitor list registration request message 1208, the FACN 220 determines whether it has stored authentication data for the mobile node 220. According to the embodiment illustrated in Figure 12 at block 1210, the FACN 220 has no authentication data associated with the mobile node 210 in this example. Because, the FACN 210 has no previous authentication data of the PDSN 232, the FACN 210 rejects the visitor list registration request and sends a visitor list registration reject reply message 1212 to the PDSN 232. In a manner similar to the visitor list registration reject reply message 1114 in Figure 11, the visitor list registration reject reply message 1212 may include a rejection reason parameter, such as an authentication data unavailable parameter. When the PDSN 232 receives the visitor list registration reject reply message 1212 from the FACN 220, the PDSN 232 queries the AAA server 1102 for the authentication data of the mobile node 210, as illustrated at the block 1214. Once the PDSN 232 receives the authentication data of the mobile node 210 from the AAA server 1102, the PDSN 232 may initiate PAP/CHAP negotiations 1216 with the mobile node 210 to establish a communication link between the mobile node 210 and the PDSN 232.

According to one embodiment, when the PDSN 232 authenticates the mobile node 210, the PDSN 232 transmits the authentication data of the mobile node 210 to the FACN 210 so that the FACN 210 can either update an existing mobile user record of the mobile node 210 with the authentication data received from the PDSN 232, or it can create a new mobile user record for the mobile node 210. In the embodiment illustrated in Figure 12, the PDSN 232 sends a visitor list registration update message 1218 including the authentication data of the mobile node 210 to

McDONNELL BOEHNEN
HULBERT & BERGHOFF
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

the FACN 220. When the FACN 220 receives the authentication data of the mobile node 210 and caches the received data into the user information record of the mobile node 210, the FACN 220 send a visitor list registration acknowledgement message 1220 to the PDSN 232, thus terminating the message sequence scenario illustrated in Figure 12. Upon a successful registration of the mobile node 210 with the PDSN 232, the mobile node 210 may start communicating data over the IP communication link.

In the situations where the mobile node 210 roams to a new radio network node that does not include the last serving PDSN within the PDSN groups defined for the new radio network node, then, the FACN 220 selects a new PDSN to service the mobile node 210. This scenario causes a communication session, such as a mobile IP communication session or an IP communication session, to be handed off to a PDSN that is not currently providing services to the mobile node 210. This scenario is referred to as a "PDSN handoff". The FACN 210 may support PDSN handoffs via a set of update messages that may be exchanged between the PDNSs and the FACN 210. Figure 13 is a block diagram of a message sequence scenario 1300 illustrating a PDSN handoff according to one embodiment. The block diagram includes the mobile node 210, the radio network node 216A, the FACN 220, an old PDSN such as the PDSN 232, a new PDSN such as the PDSN 234, and the home agent 24 of the mobile node 210. Prior to roaming to the service area of the radio network node 216A, the PDSN 232 provides network services to the mobile node 210, as illustrated at block 1302. When the mobile node 210 roams to a new service area of the radio network node 216A, the radio network node 216A sends a registration request message 1304 to the FACN 220 in order to determine a foreign agent that may provide communication services to the mobile node 210. The registration request message 1304 may include a number of parameters associated with the mobile node 210, such session specific parameters and identification data for the mobile node 210. According to the

McDONNELL BOEHNEN
HULBERT & BERGHOFF
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

embodiment illustrated in Figure 13, the PDSN 232 is not included in any of the PDSN groups associated with the radio network node 216A, so that when the FACN 220 receives the registration request message 1304, the FACN 220 selects a new PDSN, the PDSN 234, to provide services to the mobile node 210. Upon selecting the PDSN 234 for the mobile node 210, the FACN 220 sends a registration reply message 1306 including a registration rejection parameter (since the FACN 220 rejects providing registration services to the mobile node 210), and, further, includes a network address of the PDSN 234.

When the radio network node 216A receives the registration reply message 1306 from the FACN with the address of the PDSN 234, the radio network node 216A establishes a communication link such as an RP tunnel on a PPP communication link to the PDSN 234, as illustrated at block 1308. Next, the mobile node 210 sends a registration request message 1310 to the new PDSN 234 selected on the FACN 220. Since the mobile node 210 has been handed off to the new PDSN 234, the PDSN 234 does not have the mobile session associated with the mobile node 210 in its local visitor list. Thus, since the new PDSN 234 does not have authentication data of the mobile node 210, the new PDSN 234 sends a visitor list registration request message 1312 to the FACN 220 to determine if the FACN 220 has the authentication data of the mobile node 210. According to the embodiment illustrated in Figure 13, the mobile node 210 roams to the service area of the radio network node 216A from a service area of another radio network node, and thus, the mobile node 210 was previously successfully authenticated and the FACN 220 has authentication data of the mobile node 210 from a previous registration, as illustrated at block 1314. Further, if the FACN 220 determines that the mobile node is active, the FACN 220 returns the authentication data of the mobile node 210 in a visitor list registration reply message 1316. In one embodiment, the visitor list registration reply

message 1316 has a number of extension fields including the authentication data of the mobile node 210.

When the FACN 220 provides the authentication data to the new PDSN 234, the new PDSN 234 may skip AAA process and may directly register with the home agent 24. Therefore, when the new PDSN 234 receives the authentication data in the visitor list registration reply message 1316, the new PDSN 234 communicates with the home agent 24 for mobile IP re-registration request processing. The re-registration process between the new PDSN 234 and the home agent 24 may include sending a registration request message 1318 to the home agent 24, and receiving a registration reply accept message 1320 from the home agent 24 upon completing the registration process.

When the new PDSN 234 successfully registers with the home agent 24, the new PDSN 234 sends a registration reply message 1322 to the mobile node 210 indicating a completion of the registration process. Additionally, according to one embodiment of the present invention, the new PDSN 234 may send a registration update message 1324 to the FACN 220. However, since the new PDSN 234 did not use an AAA server to authenticate the mobile node 210, and instead received the authentication data of the mobile node 210 from the FACN 210, the registration update message 1324 generated on the new PDSN 234 does not have to include the authentication data received from the FACN 220. In one embodiment, if the new PDSN 234 sends the registration update message 1324 to the FACN 220, the registration update message 1324 may include a number of extension fields including session specific extensions, mobile node NAI extensions, and foreign agent-home agent authentication extensions.

When the FACN 220 receives the registration update message 1324 without the authentication data of the mobile node 210, the FACN 220 does not update its stored authentication profile for the mobile node 210. Instead, the FACN 220 marks the

McDONNELL BOEHNEN
HULBERT & BERGHOFF
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

10493645.071301

communication session specified in the message as an active session and sends a registration acknowledgement message 1326 to the FACN 220. Further, according to an exemplary embodiment, the FACN 220 uses the mobile user record associated with the mobile node 210 to determine whether the previous mobile session status has been active prior to the roaming and, whether an IP address of the last visited PDSN in the entry is different from the one specified in the registration update message 1324. According to the embodiment illustrated in Figure 13, the mobile node 210 is handed off to the new PDSN 234, and, thus, an IP address of the new PDSN 234 is different from the IP address of the last serving PDSN (the old PDSN 232). In such an embodiment, the FACN 220 sends to the last serving PDSN 232 a registration update message 1328 including an extension indicating that the mobile session of the mobile node 210 is no longer active. When the old PDSN 232 receives the registration update message 1328 from the FACN 220, the PDSN 232 may clear up the RP tunnel for the mobile session specified in the registration update message 1328 without waiting for the lifetime timer associated with the session to expire. When the old PDSN 232 receives the registration update message 1328, the old PDSN 232 sends to the FACN 220 a registration acknowledge message 1330 to indicate that the communication session has been deactivated. Upon a successful re-registration of the PDSN 234 with the home agent 24, the mobile node 210 may continue communicating data using the new PDSN 234 as a foreign agent, as illustrated at block 1330.

It should be understood that the programs, processes, methods and systems described herein are not related or limited to any particular type of computer or network system (hardware or software), unless indicated otherwise. Various types of general purpose or specialized computer systems supporting the IP networking may be used with or perform operations in accordance with the teachings described herein.

McDONNELL BOEHNEN
HULBERT & BERGHOFF
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

In view of the wide variety of embodiments to which the principles of the present invention can be applied, it should be understood that the illustrated embodiments are examples only, and should not be taken as limiting the scope of the present invention. For example, the steps of the flow diagrams may be taken in sequences other than those described, more or fewer steps may be used, and more or fewer elements may be used in the block diagrams. While various elements of the preferred embodiments have been described as being implemented in software, in other embodiments in hardware or firmware implementations may alternatively be used, and vice-versa.

The claims should not be read as limited to the described order or elements unless stated to that effect. Therefore, all embodiments that come within the scope and spirit of the following claims and equivalents thereto are claimed as the invention.

McDONNELL BOEHNEN
HULBERT & BERGHOFF
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001